Workgroup 1

Refine Safety Precepts

Precept Workgroup Out-Brief

- Workgroup Assignment
- Assumptions
- Definitions
- Top Level Mishaps (REFINED)
- TLM to Hazard Mapping
- Precepts (REFINED)
- Observations
- Issues
- Recommendations
- Path Forward

Participants

Moderator: McNeil, Josh

Scribes: Zalegowski, Frank
Mann, Ranjit (Randy)

Participants: Ericson, Clif
Rogers, Peggy
Tucker, Arthur
Muniak, Chuck
Zidzik, Jim
Garrett, Tom
Norris, Kristin & Tom Miller
Marett, Jack

Workgroup Assignment

- Review Top Level Mishaps (TLMs)
- Develop List Of Hazards
- Refine Safety Precepts
- Develop List Of Definitions Applicable To Precept Working Group
- Address Issues From Other Working Groups During The Workshop
- Conduct Out-Brief

Assumptions

- The TLMs address personal injury of public or civilians. It is the responsibility of the analyst to address personal injury of public or civilians in the TLMs that are applicable to their program.

Definitions

- ***Safety precept***
  - A guiding principle or doctrine that when followed will serve to enhance or facilitate safety. A basic truth, law or assumption, accepted as useful by the safety community, which can be used as a basis for safety reasoning in system design and operation. Good safety precepts traverse a narrow path. Their intent is to influence critical safety design guidance, yet they should not prescribe detailed design requirements that might constrain the design or the designer. In the past some safety programs have used the term safety principle; however, since principle and precept essentially have the same meaning, the team recommends the term precept to avoid confusion.

Definitions

- **Three levels of safety precepts were established for this study:**
  - **Programmatic Safety Precepts (PSPs)** – These are organizational principles and standards that will help implement safety into the system development process (i.e., safety guidance for the Program Manager that will effect mishap risk reduction through an effective safety program.)
  - **Operational Safety precepts (OSPs)** – These are operational rules that must be adhered to during system operation. They guide system design for operational use and provide the basis for design safety precepts and more detailed system safety design requirements.
  - **Design Safety Precepts (DSPs)** – These are more detailed design guidance, derived from the operational safety precepts, or other sources, and intended to facilitate safety of the system and minimize hazards.

Definitions

- ***Hazard.*** A hazard is an existing potential condition that will result in a mishap when actualized. The hazard condition is a potential state formed by the hazard source (e.g., energy) and the potential initiating mechanisms (e.g., failures) that will cause the resulting mishap and its outcome.

- ***Mishap.*** A mishap is an unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. A mishap is an actualized hazard, resulting in an undesired event with loss outcome.

Definitions

- ***Top level mishap (TLM).***
  - A TLM is the major constituent in a **categorization** method developed to help **simplify** the **tracking and classification** of many individual **hazards**. When several different hazards can result in the same type of overall mishap outcome, that generic mishap event can be classified as a TLM for the purpose of **collecting and correlating related hazards**. The TLM becomes a generic mishap category for collecting various hazards contributing to the particular outcome category in order to provide a design safety focal point. TLMs help **highlight and track major safety concerns**. TLMs **capture major safety concerns.**

UMS TLMs (REFINED)

TLM-1 Unintended/Abnormal System Mobility Operation

TLM-2 Inadvertent Firing or Release of Weapons

TLM-3 Engagement/Firing upon Unintended Targets

TLM-4 Self-Damage of Own System from Weapon Fire/Release

TLM-5 Personnel Injury

UMS TLMs (REFINED)

TLM-6 Equipment Damage

TLM-7 Environmental Damage

TLM-8 (new) – Vehicle loss

TLM-9 (new) – Vehicle collision

TLM-8 Vehicle Loss (New)

- Definition
  - The prime concern is loss or destruction of UMS vehicle due to crash into terrain, sinking, etc. Also of concern is loss of physical possession because the vehicle fails to return and ultimately crashes or is taken by 3rd party.
- Scope
  - Does not cover collision hazards which are covered by TLM-9.
- Example
  - UAV controlled flight into terrain
  - Failure of UAV propulsion system
  - USV sinks
  - UAV flies away and fails to return
  - UGV drives away and fails to return
  - UGV impacts negative terrain

TLM-9 Vehicle Collision (New)

- Definition
  - Vehicle collides with other asset. Prime concern is vehicle-to-vehicle type collisions and deconfliction of operation space considering net-centric applications.
- Scope
  - Does not include vehicle colliding with humans which are covered by TLM-1.
- Example
  - Two or more vehicles collide within their domain (operator error, Airspace violation, etc.)
  - UAV collides with manned systems (e.g. commercial airliner)
  - USV collides with commercial water craft

TLM to Hazard Mapping

No.	TLM	Causal Factors	Precepts
1.	Unintended / Abnormal System Operation	Unintended Unmanned System movement	OSP: 2, 5 DSP: 1, 2, 3, 11
		*Erroneous control (e.g. processing errors, command and control errors)	
		*Loss of command and control (e.g. 3rd party/enemy, loss of comm, interference (Jamming, RFI), cross control (video of one and control of the another))	
		Failure of weapon release subsystem results in UMS returning with ordnance in unknown state.	
		*UMS returns in unknown state	
		Unintended operation of hazardous subsystems (= generic)	OSP: 2, 3, 4, 5 DSP: 1, 2, 3, 4, 6, 7, 9, 10, 11
		Unmanned System collides with humans	OSP: 1, 2, 5 DSP: 1, 2, 3, 7
		Unmanned System collides with other vehicles with troops Move to vehicle collision (TLM -9).	OSP: 1, 2, 5 DSP: 1, 2, 3, 7
		*Insufficient/Incorrect situational awareness	OSP: 1, 5 DSP: 3, 11
		*Failure to follow operating procedures	OSP: 2, 5 DSP: 2
		*Loss of communication or communication errors (also add to TLM 8 and 9)	OSP: 1, 3 DSP: 2, 3
		Faults/damage cause Unmanned System to explode/disintegrate (move to TLM 8, 9)	OSP: 3, 4, 5 DSP: 2, 4, 5, 6, 7, 8, 9

UMS Safety Precepts (REFINED)

Proposed Program Safety Precepts (PSPs)

- PSP-1 The Program office Managing Authority will establish and maintain an SSP consistent with MIL-STD-882 or equivalent.

- PSP-2 The Program office Managing Authority will establish unifying safety precepts and processes for all programs under their cognizance to ensure:
  - Safety consistent with mission requirements, cost and schedule
  - Positive safety design features adequately mitigate all hazards presenting unacceptable mishap risk
  - Each system can be safely used in a joint warfighting environment as applicable or required.
  - That all statutory safety regulations, laws, and requirements are met

UMS Safety Precepts (REFINED)

Proposed Program Safety Precepts (PSPs)

- PSP-3 Off-the-shelf items (e.g., COTS, GOTS, NDI), re-use items, original use items, design changes, technology refresh and technology upgrades (hardware and software) are assessed for safety

- PSP-4 All life cycle phases including concept, preliminary design, detailed design, test, manufacture, deployment (to inventory), operation and disposal are addressed for safety.

- PSP-5 (new) System safety program will incorporate Top Level Mishap (TLM) approach.

UMS Safety Precepts (REFINED)

Proposed Operational Safety Precepts (OSPs)

- OSP-1 No operation will shall be executed without commensurate situational awareness
- OSP-2 The unmanned system will shall only be operated by the intended/authorized operator
- OSP-3 The unmanned system is considered unsafe until a safe state can be verified

UMS Safety Precepts (REFINED)

Proposed Operational Safety Precepts (OSPs)

- OSP-4 An unmanned system shall be in a verifiable safe state before the system is transported or weapons are loaded, powered, armed, or unloaded
- OSP-5 Weapons will shall be loaded/energized as late as possible in the operational sequence
- OSP-6 Only trained personnel using authorized procedures will shall operate and maintain unmanned combat and weapon systems

UMS Safety Precepts (REFINED)

Proposed Design Safety Precepts (DSPs)

- DSP-1 The unmanned system design shall provide positive measure to will provide safety design measures to minimize the probability risk of personnel injury during all life cycle phases.
- DSP-2 The unmanned system design shall will respond to fulfill valid authorized operator commands.
- DSP-3 The unmanned system shall will provide positive safety design measures to prevent control by anyone other than the intended operator.
- DSP-4 The unmanned system design shall will provide control and situational awareness feedback adequate to support safe operations.

UMS Safety Precepts (REFINED)

Proposed Design Safety Precepts (DSPs)

- DSP-5 There shall be The unmanned system will provide safety design measures to isolate power from weapons or ordnance initiation circuits until intent to initiate.

- DSP-6 The unmanned system design shall will prevent firing of weapons into unmanned system structure or other weapons. and minimize hazards to personnel, equipment, and other vehicle weapons from missile exhaust, gun blast or ejecta.

- DSP-7 The A unmanned system shall will mitigate through design measures the uncommanded fire/release of weapons or radiation of hazardous emitters.

- DSP-8 There shall be positive_The unmanned system will provide safety design measures to monitor and protect against hazardous system mode combinations.

UMS Safety Precepts (REFINED)

Proposed Design Safety Precepts (DSPs)

- DSP-9 There shall be positive The unmanned system will provide safety design measures for an authorized operator to abort a weapon fire sequence or return the system to a safe state
- DSP-10 There shall be positive The unmanned system will provide safety design measures for an authorized operator to safely change states and modes
- DSP-11 The unmanned system safety critical software shall will preclude unintended/non-required functionality

UMS Safety Precepts (REFINED)

Proposed Design Safety Precepts (DSPs)

- DSP-12 There shall be positive The unmanned system will provide safety design means (for an authorized operator) to identify the state of an unmanned system.
- DSP-13 An The unmanned system shall will mitigate, through design, single point (preferably double point) or common mode failures for high (catastrophic) and serious (critical) risks.
- DSP-14 The unmanned system will minimize the use of hazardous materials. will be minimized.
- DSP-15 There shall be positive The unmanned system will provide safety design measures to prevent exposure of personnel to the hazards of high voltage, toxic materials, excessive noise levels, and other known environments created by unmanned system equipment.

UMS Safety Precepts (REFINED)

Proposed Design Safety Precepts (DSPs)

- DSP-16 There shall be positive measures The unmanned system will provide safety design to prevent the exposure of unmanned system personnel, ordnance or equipment to unsafe levels of radio frequency (RF), X-ray, or laser radiation

- DSP – 17 (new) The unmanned system will minimize hazards to personnel, equipment, from exhaust, gun blast or ejecta.

- DSP – 18 (new) The unmanned system will initialize/re-initialize in a known safe state.

Observations

- Some or all TLMs and precepts may be applicable to manned systems as well as unmanned systems.

Issues

- Insufficient time to refine definitions.
- Address return of contaminated (NBC) vehicle.
- Does DSP-2 address a safety issue? Do we need it?
- Why are there different Risk Acceptance Authority Levels between Agencies?
- PSP-2 item 3 may not be applicable to all programs. Need guidance on tailoring precepts.
- Do we need PSPs to use TLMs (developed here) in developing SSPP?

Issues (continued)

- Need to resolve difference between “Authorized” and “Intended” operator.
- Refer DSP-13, need to resolve risk issues between Services, Agencies, etc.
- Are DSPs, OSPs, and PSPs provided as guidance or requirements?
- Investigate changing TLM name to:
  - Safety critical event
  - Top level safety event

Recommendations:

- Refine TLM to Hazard mapping
- TLMs should be tailored for each system
- Communicate TLMs and Precepts to broader safety community
- Incorporate TLM and precepts approach into MIL-STD-882 and equivalent
- Recommend a working group to continue finalization of definitions.

Path Forward

- Reconvene (subset) of Work Group 1
  - Revise and finalize TLM list.
  - Complete mapping:
    TLMs →Hazards →Precepts
  - Review mapping for missing precepts.

Provide List of Recommended Precepts for OSD Standard